

DOCKET NO: 240204US28

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

IN RE APPLICATION OF :  
TETSURO MOTOYAMA : EXAMINER: SIKRI, ANISH  
SERIAL NO: 10/670,604 :  
FILED: SEPTEMBER 26, 2003 : GROUP ART UNIT: 2143  
FOR: METHOD AND SYSTEM FOR :  
SUPPORTING MULTIPLE PROTOCOLS  
USED TO MONITOR NETWORKED  
DEVICES IN A REMOTE MONITORING  
SYSTEM

APPEAL BRIEF

COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

SIR:

Applicants appeal the outstanding Final Rejection of October 5, 2007, finally  
rejecting each of pending Claims 1-36.

I. REAL PARTY IN INTEREST

The above-noted application is assigned to Ricoh Company, Ltd., which is the real  
party in interest, having a place of business at Tokyo, Japan.

II. RELATED APPEALS AND INTERFERENCES

Applicants and Applicants' representative are not aware of any related appeals or  
interferences that will directly effect or be directly affected by or having a bearing on the  
Board's decision in the pending appeal.

### III. STATUS OF CLAIMS

Claims 1-36 are pending in this application and the rejection of each of Claims 1-36 is being appealed.

### IV. STATUS OF AMENDMENTS

An Amendment was filed on August 1, 2007, in response to the non-final Rejection mailed June 1, 2007. This amendment was entered. A Request for Reconsideration was filed on December 10, 2007. Accordingly, all previously filed Amendments have been considered by the Examiner and are reflected in the attached claims.

### V. SUMMARY OF CLAIMED SUBJECT MATTER

The applicants of the present application have recognized that it is desirable to monitor hardware devices that are located on a network for maintenance, usage, or other purposes. However, in view of manufacturer differences relating to hardware devices and interfaces, it may be difficult for a monitoring device to communicate with various other devices connected to a network. Such a disadvantage most likely prevents network administrators from obtaining crucial information about the performance and efficiency of the devices connected to the network.<sup>1</sup>

It is possible that different protocols require their own set of additional information before they can be used to access a monitored device. For example, a SNMP device may have a community name associated with it. This community name may be different from another device. Therefore, the monitoring device needs to obtain the community name before it can access the monitored device. Another example is that HTTP may be on a secure

---

<sup>1</sup> Specification, page 4, lines 6-11.

channel that requires a login name and password. The monitoring device would need to obtain the login name and password in order to access the monitored device using HTTP.

The exemplary embodiments described in the specification are directed toward a system that is easily adaptable to use multiple protocols to access monitored devices. Advantageously, additional protocols can be easily added to the system by supplying access to the additional information corresponding to the additional protocols.

It is noted that the specification states, “[f]or the purposes of this patent application, the inventor has determined that a hardware device that is controlling, configuring, or monitoring the plurality of distinct devices or hardware devices would be referred to as a monitoring device and the hardware devices that are being controlled, configured, or monitored by the monitoring device would be referred to as ‘monitored devices.’”<sup>2</sup>

Claim 1 is directed toward method of monitoring a monitored device among distinct devices communicatively coupled to a network. Claim 1 is generally supported by Figs. 1 (overall system diagram), 9 (overall system diagram), and 25 (flow chart depicting the steps of monitoring a network device using multiple protocols). A monitored device and a monitoring device are defined in the specification as noted above. Fig. 1 shows monitored devices 24, 28, 32, and 17 (for example). Fig. 9 shows monitored devices 908 and 910, for example. Fig. 9 shows monitoring station 902. As shown in Fig. 9, monitoring station 902 is communicatively coupled to network 100, along with the monitored devices.

Claim 1 recites retrieving by the monitoring computer, from a first memory, information for accessing the monitored device using at least one communication protocol supported by the monitored device. Page 12, lines 8-21 of the specification describes different databases that may be used, and the memory that may store the databases. Controller 902 of Fig. 9 (which is a monitoring computer, see page 22, lines 10-11) is

---

<sup>2</sup> Specification, page 4, lines 1-5.

communicatively coupled to storage device 904 and database 906.<sup>3</sup> “The storage device 904 preferably stores detailed information about each of the monitored devices 908-914. For example, detailed information, such as the make, model, and various functions and troubleshooting details of the laser printer 908 are stored in the storage device 904.”<sup>4</sup> The monitoring device can use multiple protocols (HTTP, FTP, and SNMP, for example) to monitor devices.<sup>5</sup>

Exemplary embodiments of the monitoring device include monitor service module 1004, which may obtain an IP address (exemplary information for accessing the monitored device).<sup>6</sup>

“Figure 19 illustrates the organization of the monitor database, which includes the device information for each monitored device (see also Table I). As shown in figure 19, a set of parameters, one set for each communication protocol (e.g., SNMP, HTTP, and FTP), is associated with the device information DeviceInfo 1902 for each monitored device. Moreover, each set of parameters for a particular protocol (e.g., SNMP 1908, HTTP 1910, and FTP 1912) is organized as a list of parameter name and value pairs, e.g., sPar1Name and sPar1Value. Note that the number of parameters for each protocol may be shorter or longer than the number shown in figure 19. For example, a username and password may be stored as FTP parameters, while a community name and a password may be stored as SNMP parameters for a given monitored device. As shown in figure 19, the monitor database also includes information related to the DeviceHistory 1904 and the EnumCorrespondence 1906.”<sup>7</sup>

---

<sup>3</sup> Specification, page 23, lines 7-8.

<sup>4</sup> Specification, page 23, lines 12-14.

<sup>5</sup> Specification, page 23, lines 21-26

<sup>6</sup> Specification, page 24, lines 9-13.

<sup>7</sup> Specification, page 31, line 32 to page 32, line 9.

In an exemplary embodiment, the first memory is the monitor database 1014, which contains the device information shown in Fig. 19.<sup>8</sup>

Claim 1 also recites storing by the monitoring computer, in a second memory, the information for accessing the monitored device retrieved from the first memory. Figure 18 illustrates the map structure 1800 used to pass a vector of parameters for each protocol obtained from the monitor database (exemplary first memory)<sup>9</sup> to a software object associated with each monitored device (exemplary second memory). The map structure 1800 associates each protocol/key field 1802, 1804, and 1806, with a corresponding vector of parameters 1808, 1810, and 1812, respectively, arranged according to the SParameter format shown in figure 17. For example, for the SNMP protocol 1802, the vector of parameters 1808 may include a list of parameter name, parameter value pairs that are used to access the monitored device with the SNMP protocol. For example, the SNMP parameter names stored in the vector 1808 might include "Community Name" and "Password", together with the corresponding parameter values. Note, however, that the organization of the map structure 1800 allows for any number of protocols and associated parameter vectors, and is not limited to the SNMP, HTTP, and FTP protocols shown in figure 18.<sup>10</sup>

In an exemplary embodiment, the information for accessing the device obtained from the first memory is stored in a second memory. In this exemplary embodiment, the second memory comprises a vector of parameter name and parameter value pairs for each of the plurality of communication protocols. Moreover, in this exemplary embodiment, the information for accessing the device is stored in a software object associated with the device.<sup>11</sup>

---

<sup>8</sup> Specification, page 36, lines 28-31.

<sup>9</sup> See, Figs. 20-22, and there corresponding description in the specification.

<sup>10</sup> Specification, page 32, lines 14-25.

<sup>11</sup> Specification, page 37, lines 3-7, and Fig. 13.

Claim 1 also recites selecting by the monitoring computer a communication protocol among the plurality of communication protocols, the monitored device being configured to process two or more of the plurality of communication protocols. Page 5, line 31 to page 6, line 7, describes how SNMP, FTP, and HTTP may be used in succession to obtain information from a monitored device. Thus, the monitored device is able to process two or more of a plurality of communication protocols. Furthermore, this step is shown in step 2506 of Fig. 25.

Claim 1 also recites directly accessing the monitored device using the selected communication protocol and the information retrieved from the first memory and stored in the second memory by the monitoring computer. It is noted that this step is shown in step 2508 of Fig. 25. Also, figure 14 shows the sequence of the status monitor function to determine the status of a monitored device by the MonitorManager module 1102, as illustrated in figure 11. Furthermore, Fig. 9 shows an example of protocol commands 950 being transmitted from monitoring station 902 to monitored devices (i.e., laser printer 908).

Claim 13 describes a system for storing information configured to be used for a plurality of communication protocols to access a monitored device by a monitoring computer among distinct devices communicatively coupled to a network. Claim 13 is written in means-plus-function language, and recites functionality similar to what is recited in method Claim 1. Thus, support for Claim 13 is similar to what was identified for Claim 1. While Claim 13 is discussed below, information stated for Claim 1, that applies to Claim 13, will not be repeated.

Claim 13 recites means for retrieving, from a first memory, information for accessing the monitored device using at least one communication protocol supported by the monitored device, said means for retrieving being disposed in the monitoring computer. Fig. 8 shows an exemplary computer structure that may be used to monitor a device. Fig. 8 includes CPU

362, which may execute the algorithms discussed in the specification (see discussion of Figs. 11, 13, and 14, for example). Fig. 8 also shows also a plurality of interfaces for communication with other devices (i.e., 366, 378, 382, 386, and 398). The functionality is supported by at least the sections of specification identified for Claim 1.

Claim 13 also recites means for storing, in a second memory, the information for accessing the monitored device retrieved from the first memory, said means for storing being disposed in the monitoring computer. The means for storing can be the above-noted CPU, which causes information to be stored in the second memory, for example. The functionality is supported by at least the sections of specification identified for Claim 1.

Claim 13 also recites means for selecting a communication protocol among the plurality of communication protocols, said means for selecting being disposed in the monitoring computer, the monitored device being configured to process two or more of the plurality of communication protocols. Again, CPU 362 is capable of selecting the protocol to be used to communicate with the monitored device. As explained with respect to Fig. 16, “the CDeviceODBC class can handle as many protocols and their associated parameter names and values through the pointer to the CAbsProtocolParameter type, without identifying the protocol. The obtained information for each device (e.g., IP Address) is stored in the data structure of FIG. 18 and passed to the MonitorManager module 1102 through the obtainConfig function. From the CDeviceODBC perspective, all the objects used to obtain the protocol name and the associated parameter names and values are considered to be a type of CAbsProtocol Parameters. When a new parameter is added, therefore, the new object should be created and stored in the vector of pointers to CAbsProtocolParameters class.”<sup>12</sup> The functionality is supported by at least the sections of specification identified for Claim 1.

---

<sup>12</sup> Specification, page 35, lines 11-19.

Claim 13 also recites means for accessing the monitored device using the selected communication protocol and the information retrieved from the first memory and stored in the second memory disposed in the monitoring computer. Again, it is note that Fig. 18 shows a plurality of different interfaces and a CPU that can access the monitored device. The functionality is supported by at least the sections of specification identified for Claim 1.

Independent Claim 25 recites elements analogous to those of Claim 1. Claim 25 is directed toward a computer readable storage medium encoded with instructions which when executed by a processing apparatus causes the processing apparatus to implement a method analogous to Claim 1. Page 38, lines 1-6, provides support for the claimed “computer readable storage medium.” The method recited in Claim 25 is supported by at least the same portions of the specification identified in the discussion of Claim 1.

#### VI. GROUND OF REJECTION TO BE REVIEWED ON APPEAL

The sole ground of rejection being appealed is whether Claims 1-36 are anticipated by Ramberg et al. (U.S. Patent Publication No. 2003/0014505, hereinafter Ramberg).

#### VII. ARGUMENT

Claim 1 is patentable over Ramberg because, as noted below, Ramberg does not disclose or suggest every element of Claim 1.

##### The MIB of Ramberg is not a Monitoring Device

The Advisory Action mailed January 2, 2008 clearly indicates that the position of the Office is that the “MIB is the monitoring device.”<sup>13</sup> This position is respectfully traversed.

The present specification defines “monitoring device” as “a hardware device that is controlling, configuring, or monitoring the plurality of distinct devices or hardware

---

<sup>13</sup> Advisory Action, January 2, 2008, continuation sheet.



devices.”<sup>14</sup> An MIB does not control, configure, or monitor a plurality of distinct devices or hardware devices. An MIB (management information base) defines a collection of objects to be collected.<sup>15</sup> Paragraphs [0038] and [0039] of Ramberg merely describe information defined in the MIB. The MIB does not meet the above-noted definition of a monitoring device.

Also, the MIB of Ramberg does not perform the claimed steps of:

retrieving *by the monitoring computer*, from a first memory, information for accessing the monitored device using at least one communication protocol supported by the monitored device...

selecting *by the monitoring computer* a communication protocol among the plurality of communication protocols, the monitored device being configured to process two or more of the plurality of communication protocols; and

directly accessing the monitored device using the selected communication protocol and the information retrieved from the first memory and stored in the second memory *by the monitoring computer*.

#### The Remote Computer of Ramberg is not the Claimed Monitoring Computer

If the Office were to change its position during the appeal to argue that the Remote Computer 120 of Ramberg is a “monitoring computer,” the Office would still be incorrect.

The remote computer 120 of Ramberg does not perform the claimed

retrieving by the monitoring computer, from a first memory, information for accessing the monitored device using at least one communication protocol supported by the monitored device;

storing by the monitoring computer, in a second memory, the information for accessing the monitored device retrieved from the first memory; [and]

---

<sup>14</sup> Specification, page 4, lines 1-5.

<sup>15</sup> Specification, page 4, lines 22-26.

selecting by the monitoring computer a communication protocol among the plurality of communication protocols, the monitored device being configured to process two or more of the plurality of communication protocols.

The remote computing system 120 of Ramberg uses only one communication protocol, that being SNMP. Paragraph [0007] of Ramberg describes that the communication between the remote service technician's computer and the ADC device platform is SNMP. The HTTP protocol discussed in paragraph [0007] is for communications between the remote computing system and an HTTP server. However, only SNMP is used between the remote computing system of the technician and the ADC 100. In Ramberg, the web browser is used as a front end of the remote computing system of the technician, but SNMP is used to communicate with the ADC 100. Particularly, paragraph [0007] states

In each ADC device platform of the plurality of the ADC device platforms, **a Simple Network Management Protocol ("SNMP") master agent communicates with the service technician's remote computing system.** An SNMP subagent translates a diagnostic query forwarded by the SNMP master agent into a format suitable for reception by the subsystem to which the query was directed. The SNMP subagent translates data received from the queried subsystem into the proper format for transmission to the SNMP master agent which forwards the data to the remote computing system. Once the data arrives at the remote computing system, it may be analyzed by the service technician.

Thus, the remote computing system used by the technician in Ramberg does not select a communication protocol among the plurality of communication protocols. There is only one protocol available and the claimed "selecting" is not performed.

Moreover, paragraph [0030] of Ramberg states "According to one embodiment of the invention, the remote service technician's web browser uses Java applets as the user interface **and SNMP to communicate with ADC device platforms**" (emphasis added).

Moreover, paragraph [0024] of Ramberg describes the remote computing system used by the technician, which states

**The remote service technician sends commands for controlling the ADC device platform over the communications network, such as the World Wide Web, through the network communications device to the ADC device platform. Commands passing over the communications network may arrive at the ADC device platform in a communications format different from the format required by the ADC devices connected to the ADC device platform. Various subsystems on the ADC device platform translate information within the ADC device platform into appropriate communication formats (emphasis added).**

Furthermore, the monitored device (ADC device 101 or 102) of Ramberg is not configured to process two or more of the plurality of communication protocols. On the contrary, ADC devices 101 and 102 each have their own format and the SNMP master agent and SNMP subagent translate the query to the particular format of the ADC device 101 or 102.<sup>16</sup> Thus, ADC device 101 or 102 is not configured to process two or more of the plurality of protocols, and is only configured to process one protocol. Thus, the claimed “the monitored device being configured to process two or more of the plurality of communication protocols” is not disclosed or suggested by Ramberg.

Claim 1 also recites “directly accessing the monitored device using the selected communication protocol and the information retrieved from the first memory and stored in the second memory by the monitoring computer.” The remote computing system 120 does not directly access the monitored device (ADC device 101 or 102). On the contrary, any query sent by the remote computer of Ramberg needs to be relayed through the SNMP master agent 220 before the query is sent to the ADC device 101 or 102. This is because the ADC device only processes data in one communication protocol, and the SNMP master agent has to convert the format of the query into SNMP and the SNMP subagent has to convert the SNMP into the one communication protocol used by ADC device 101 or 102. Thus, the

---

<sup>16</sup> Ramberg, paragraph [0025].

remote computer 120 does not directly access the monitored device (ADC device 101 or 102).

Monitored Devices 101 and 102 of Ramberg are not directly accessed by a monitoring device

ADC 101 and 102 are not directly accessed by the MIB. The MIB is database definition of object collection, and does not directly access anything.

Ramberg describes a system and method for remotely diagnosing and repairing a plurality of automatic data collection devices 101 and 102.<sup>17</sup> A service technician utilizes a web browser in a remote computing system to access a Hypertext Transfer Protocol ("HTTP") server and retrieve from the HTTP server Hypertext Mark-Up Language ("HTML") documents, Dynamic Hypertext Mark-Up Language ("DHTML") documents, Extensible Mark-Up Language ("XML") documents, and/or documents in other data formats over the World Wide Web. The service technician's remote computing system uses small diagnostic programs, or applets, contained in the HTML documents, DHTML documents, and/or XML documents to perform diagnostic queries on ADC device platforms, diagnose anomalies, and reconfigure malfunctioning subsystems on the ADC device platform. In each ADC device platform of the plurality of the ADC device platforms, a Simple Network Management Protocol ("SNMP") master agent communicates with the service technician's remote computing system. An SNMP subagent translates a diagnostic query forwarded by the SNMP master agent into a format suitable for reception by the subsystem to which the query was directed. The SNMP subagent translates data received from the queried subsystem into the proper format for transmission to the SNMP master agent which forwards the data to the

---

<sup>17</sup> Ramberg, Abstract and paragraph [0034].

remote computing system. Once the data arrives at the remote computing system, it may be analyzed by the service technician.<sup>18</sup>

The remote computing system 120 does not directly access the monitored device (ADC device 101 or 102). On the contrary, any query sent by the remote computer of Ramberg needs to be relayed through the SNMP master agent 220 before the query is sent to the ADC device 101 or 102. This is because the ADC device 101 or 102 only processes data in one communication protocol, and the SNMP master agent has to convert the format of the query into SNMP and the SNMP subagent has to convert the SNMP into the one communication protocol used by ADC device 101 or 102. Thus, the remote computer 120 does not directly access the monitored device (ADC device 101 or 102).

The Monitored Device in Ramberg is not Configured to Process two or more Communication Protocols

The monitored device (ADC device 101 or 102) of Ramberg is not configured to process two or more of the plurality of communication protocols. On the contrary, ADC device 101 or 102 each has its own format and the SNMP master agent and SNMP subagent translate a query to the particular format of the ADC device 101 or 102.<sup>19</sup> Thus, ADC device 101 or 102 is not configured to process two or more of the plurality protocols, and is only configured to process one protocol.

Thus, Ramberg does not disclose or suggest the claimed “the monitored device being configured to process two or more of the plurality of communication protocols.”

Ramberg does not Disclose or Suggest the First Memory and the Second Memory

Claim 1 recites, *inter alia*,

---

<sup>18</sup> Ramberg, paragraph [0007].

<sup>19</sup> Ramberg, paragraph [0025].

retrieving by the monitoring computer, from a first memory, information for accessing the monitored device using at least one communication protocol supported by the monitored device;

storing by the monitoring computer, in a second memory, the information for accessing the monitored device retrieved from the first memory.

The Final Rejection, when rejecting Claim 1, refers to the MIB in the ADC device platform with respect to the first and second memories. As indicated by the different names, the first memory and second memory are different. Exemplary embodiments show that the first memory is database 1014, and that the second memory is a software object.<sup>20</sup> The one MIB in the ADC device platform does not equate to the claimed “first memory” and “second memory.”

Thus, Ramberg does not disclose or suggest the claimed “first memory” and “second memory.”

#### The Office has Failed to Properly Construe the Claims

Page 19 of the Final Rejection mischaracterizes the law, by stating

In response to applicant’s argument that 1, 13, and 25, [sic] a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

It is noted that the Office Action provides no citations in support of this proposition. It is well established that each word of every claim must be given weight. See, In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

---

<sup>20</sup> Specification, page 36, line 28 to page 37, line 7.

Claims 1, 13, and 25 do not recite an intended use. On the contrary, elements of Claims 1, 13, and 25 are defined functionally, which is an acceptable way to clearly describe and distinctly claim the subject matter regarded as the invention.

Controlling precedent does not support the conclusion that a claimed function can be ignored as the PTO attempts to do here. In this regard, In re Schreiber, 128 F.3d 1473, 1477-78 44 USPQ 2d 1429, 1431-32 (Fed. Cir. 1999) (cited as authority in MPEP §2114 ) does not support any theory that functional limitations can be ignored, rather this case requires that a reference structure used to reject a claim structure defined by what it does must INHERENTLY perform the claimed function. In this regard, it is well established that inherency requires **the certainty that something will happen**, not merely a possibility or even a probability that something may occur. See In re Robertson, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) and In re Oelrich, 212 USPQ 323, 326 (CCPA 1981).

Note the further discussion of functional limitations in MPEP §2173.05(g) that specifically treats the Swinehart decision (In re Swinehart 439 F.2d 210, 169 USPQ 226 (CCPA 1971)) mentioned in MPEP §2114 as noting that functional limitations defining structure by the function performed by that structure are valid claim limitations that this section instructs “must be evaluated and considered, just like any other limitation of the claim . . . .”

Moreover, Claim 13 is a means plus function claim, which has not been properly treated. The required analysis of the base Claim 13 recited “means” and associated functions has not been performed. In this regard, the PTO reviewing court recently emphasized that conclusory findings that omit analysis as to “means” claim limitations are improper in Gechter v. Davidson 43 USPQ2d 1030, 1035 (Fed. Cir. 1997) as follows:

In addition, the [PTO] never construed the scope of the structures disclosed in the specification for the claimed "receiving means," nor did the [PTO] expressly find that the "receiving means" disclosed in the specification was

structurally equivalent to that embodied in [the reference].  
Moreover, the [PTO] also failed to define the exact function of  
the receiving means, as well as to find that [the reference]  
disclosed the identical function. [Emphasis added, citation  
omitted.]

In view of the above-noted deficiencies in Ramberg, Applicants respectfully submit  
that Claim 1 (and any claims dependent thereon) patentably distinguish over Ramberg.

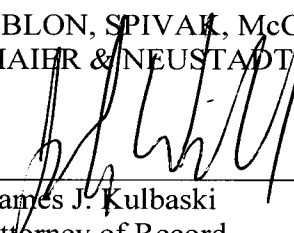
Independent Claims 13 and 25 recite limitations analogous to the limitations recited in  
Claim 1. Accordingly, for at least the reasons stated above for the patentability of Claim 1,  
Applicants respectfully submit that Ramberg does not anticipate Claims 13 and 15 (and any  
claims dependent thereon).

#### VIII. CONCLUSION

For the foregoing reasons, Applicants respectfully submits that each of Claims 1-36  
patentably distinguish over Ramberg.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

  
\_\_\_\_\_  
James J. Kulbaski  
Attorney of Record  
Registration No. 34,648

Customer Number  
**22850**

Tel: (703) 413-3000  
Fax: (703) 413 -2220  
(OSMMN 08/07)

Joseph Wrkich  
Registration No. 53,796



CLAIMS APPENDIX

1. (Rejected). A method of storing information configured to be used for a plurality of communication protocols to access a monitored device by a monitoring computer among distinct devices communicatively coupled to a network, comprising:

retrieving by the monitoring computer, from a first memory, information for accessing the monitored device using at least one communication protocol supported by the monitored device;

storing by the monitoring computer, in a second memory, the information for accessing the monitored device retrieved from the first memory;

selecting by the monitoring computer a communication protocol among the plurality of communication protocols, the monitored device being configured to process two or more of the plurality of communication protocols; and

directly accessing the monitored device using the selected communication protocol and the information retrieved from the first memory and stored in the second memory by the monitoring computer.

2. (Rejected). The method of claim 1, wherein the retrieving step comprises: accessing a memory external to a monitoring computer to obtain the information for accessing the monitored device.

3. (Rejected). The method of claim 1, wherein the selecting step comprises: selecting a communication protocol among SNMP, HTTP, and FTP.

4. (Rejected). The method of claim 1, wherein the retrieving step comprises:  
retrieving, from the first memory, at least one of a username and a password for accessing the  
monitored device using FTP.

5. (Rejected). The method of claim 1, wherein the retrieving step comprises:  
retrieving, from the first memory, at least one of a community name and a password for  
accessing the monitored device using SNMP.

6. (Rejected). The method of claim 1, wherein the retrieving step comprises:  
retrieving, from the first memory, an IP address of the monitored device.

7. (Rejected). The method of claim 1, wherein the second memory comprises a vector  
of parameter name and parameter value pairs for each of the plurality of communication  
protocols.

8. (Rejected). The method of claim 1, wherein the storing step comprises: storing the  
information for accessing the monitored device in a device software object associated with  
the monitored device.

9. (Rejected). The method of claim 8, wherein the device software object is stored in  
a random-access memory unit of the monitoring computer.

10. (Rejected). The method of claim 1, wherein the retrieving step comprises:  
accessing the first memory using virtual functions associated with an abstract software class.

11. (Rejected). The method of claim 1, wherein the accessing step comprises:  
transmitting to the monitored device, information stored in the second memory necessary to  
access the monitored device using the selected communication protocol.

12. (Rejected). The method of claim 11, wherein the accessing step comprises:  
receiving, by the monitored device, the transmitted information; and processing, by the  
monitored device, the received information.

13. (Rejected). A system for storing information configured to be used for a plurality  
of communication protocols to access a monitored device by a monitoring computer among  
distinct devices communicatively coupled to a network, comprising:

means for retrieving, from a first memory, information for accessing the monitored  
device using at least one communication protocol supported by the monitored device, said  
means for retrieving being disposed in the monitoring computer;

means for storing, in a second memory, the information for accessing the monitored  
device retrieved from the first memory, said means for storing being disposed in the  
monitoring computer;

means for selecting a communication protocol among the plurality of communication  
protocols, said means for selecting being disposed in the monitoring computer, the monitored  
device being configured to process two or more of the plurality of communication protocols;  
and

means for accessing the monitored device using the selected communication protocol  
and the information retrieved from the first memory and stored in the second memory  
disposed in the monitoring computer.

14. (Rejected). The system of claim 13, wherein the means for retrieving comprises:  
means for accessing a memory external to a monitoring computer to obtain the information  
for accessing the monitored device.

15. (Rejected). The system of claim 13, wherein the means for selecting comprises:  
means for selecting a communication protocol among SNMP, HTTP, and FTP.

16. (Rejected). The system of claim 13, wherein the means for retrieving comprises:  
means for retrieving, from the first memory, at least one of a username and a password for  
accessing the monitored device using FTP.

17. (Rejected). The system of claim 13, wherein the means for retrieving comprises:  
means for retrieving, from the first memory, at least one of a community name and a  
password for accessing the monitored device using SNMP.

18. (Rejected). The system of claim 13, wherein the means for retrieving comprises:  
means for retrieving, from the first memory, an IP address of the monitored device.

19. (Rejected). The system of claim 13, wherein the second memory comprises a  
vector of parameter name and parameter value pairs for each of the plurality of  
communication protocols.

20. (Rejected). The system of claim 13, wherein the means for storing comprises:  
means for storing the information for accessing the monitored device in a device software

object associated with the monitored device.

21. (Rejected). The system of claim 20, wherein the device software object is stored in a random-access memory unit of the monitoring computer.

22. (Rejected). The system of claim 13, wherein the means for retrieving comprises: means for accessing the first memory using virtual functions associated with an abstract software class.

23. (Rejected). The system of claim 13, wherein the means for accessing comprises: means for transmitting to the monitored device, information stored in the second memory necessary to access the monitored device using the selected communication protocol.

24. (Rejected). The system of claim 23, wherein the means for accessing comprises: means for receiving, by the monitored device, the transmitted information; and means for processing, by the monitored device, the received information.

25. (Rejected). A computer readable storage medium encoded with instructions which when executed by a processing apparatus cause the processing apparatus to implement a method of storing information configured to be used for a plurality of communication protocols to access a monitored device by a monitoring computer among distinct devices communicatively coupled to a network, the method comprising:

retrieving by the monitoring computer, from a first memory, information for accessing the monitored device using at least one communication protocol supported by the monitored device;

storing by the monitoring computer, in a second memory, the information for accessing the monitored device retrieved from the first memory;

selecting by the monitoring computer a communication protocol among the plurality of communication protocols, the monitored device being configured to process two or more of the plurality of communication protocols; and

accessing the monitored device using the selected communication protocol and the information retrieved from the first memory and stored in the second memory by the monitoring computer.

26. (Rejected). The computer readable storage medium of claim 25, wherein the retrieving comprises: accessing a memory external to a monitoring computer to obtain the information for accessing the monitored device.

27. (Rejected). The computer readable storage medium of claim 25, wherein the selecting comprises: selecting a communication protocol among SNMP, HTTP, and FTP.

28. (Rejected). The computer readable storage medium of claim 25, wherein the retrieving comprises: instructions for retrieving, from the first memory, at least one of a username and a password for accessing the monitored device using FTP.

29. (Rejected). The computer readable storage medium of claim 25, wherein the retrieving comprises: retrieving, from the first memory, at least one of a community name and a password for accessing the monitored device using SNMP.

30. (Rejected). The computer readable storage medium of claim 25, wherein the retrieving comprises: retrieving, from the first memory, an IP address of the monitored device.

31. (Rejected). The computer readable storage medium of claim 25, wherein the storing comprises: storing, in the second memory, a vector of parameter name and parameter value pairs for each of the plurality of communication protocols.

32. (Rejected). The computer readable storage medium of claim 25, wherein the storing comprises: storing the information for accessing the monitored device in a device software object associated with the monitored device.

33. (Rejected). The computer readable storage medium of claim 32, wherein the method further comprises: storing the device software object is-in a random-access memory unit of the monitoring computer.

34. (Rejected). The computer readable storage medium of claim 25, wherein the retrieving comprises: accessing the first memory using virtual functions associated with an abstract software class.

35. (Rejected). The computer readable storage medium of claim 25, wherein the accessing comprises: transmitting to the monitored device, information stored in the second memory necessary to access the monitored device using the selected communication protocol.

36. (Rejected). The computer readable storage medium of claim 35, wherein the accessing comprises: receiving, by the monitored device, the transmitted information; and processing, by the monitored device, the received information.



EVIDENCE APPENDIX

None

RELATED PROCEEDING APPENDIX

None